

# COMPUTING AUTOMORPHISM GROUPS OF RATIONAL FUNCTIONS

XANDER FABER, MICHELLE MANES, AND BIANCA VIRAY

**ABSTRACT.** Let  $\phi$  be an endomorphism of the projective line of degree at least 2, defined over a noetherian commutative ring  $R$  with unity. We show that the automorphism group of  $\phi$  is a finite group scheme, and we construct algorithms to compute it when  $R$  is a finite field or a number field. We also give an algorithm for determining when two such endomorphisms are conjugate. We have implemented these algorithms in Sage when  $R$  is a finite field or the field of rational numbers.

## 1. INTRODUCTION

Let  $F$  be a field, and let  $\phi = f/g \in F(z)$  be a rational function such that  $\gcd(f, g) = 1$  and  $d = \deg(\phi) := \max\{\deg(f), \deg(g)\} > 1$ . When viewed as an endomorphism of the projective line  $\phi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$ , a dynamical theory of  $\phi$  arises from iteration. That is, for  $x \in \mathbb{P}_F^1$ , we may consider its orbit

$$x \mapsto \phi(x) \mapsto \phi^2(x) \mapsto \phi^3(x) \mapsto \cdots$$

(Here we write  $\phi^1 = \phi$  and  $\phi^n = \phi \circ \phi^{n-1}$  for each  $n > 1$ .) The case  $F = \mathbb{C}$  — dynamics of self-maps of the Riemann sphere — has a fascinating history dating back as far as Newton; e.g., see [1, 11]. When  $F$  is a finite field, these dynamical systems behave (conjecturally) like random maps, which has applications to factoring integers [13, 2]. If  $F$  is a number field, then we have the younger theory of arithmetic dynamics [15]. The case where  $F$  is a non-Archimedean field is younger still and draws much inspiration from the complex case [3, 10].

In the present paper, we study algorithmic aspects of a fundamental question:

When do two rational functions  $\phi, \psi \in F(z)$  exhibit the same dynamical behavior?

For topological reasons, they must have the same degree. Given any fractional linear transformation  $f(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$ , viewed as an element of  $\mathrm{PGL}_2(F)$ , the dynamical behavior of  $\phi$  is equivalent to that of  $\phi^f := f \circ \phi \circ f^{-1}$ ; indeed,  $f$  maps the  $\phi$ -orbit of a point  $x \in \mathbb{P}_F^1$  to the  $\phi^f$ -orbit of  $f(x)$ . If there exists  $f \in \mathrm{PGL}_2(F)$  such that  $\psi = f \circ \phi \circ f^{-1}$ , then we say that  $\phi$  and  $\psi$  are **conjugate** (over  $F$ ). Conjugation defines an action of  $\mathrm{PGL}_2(F)$  on the parameter space of rational functions of fixed degree  $d > 1$ , denoted  $\mathrm{Rat}_d(F)$ . The stabilizer of a rational function  $\phi$  for this action is called the **automorphism group** of  $\phi$ , and is denoted by  $\mathrm{Aut}_\phi(F)$ . This group is always finite, and it is trivial for most rational functions.

---

*Date:* February 28, 2012.

The first and second authors were partially supported by NSF grants DMS-0902532 and DMS-1102858, respectively. The third author was partially supported by NSF grant DMS-1002933 and by ICERM.

We thus have two problems which happen to be computationally quite similar: (1) determine whether two given rational functions are conjugate, and (2) determine whether a given rational function has nontrivial automorphism group. We focus mainly on algorithms designed to compute automorphism groups, and in the final section we sketch the modifications needed to address the first problem.

We design three algorithms for computing automorphism groups of rational functions, each applying to a slightly different setting. Let  $F$  be a field and  $\phi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$  be a morphism of degree at least 2, as above. Our first algorithm computes the absolute automorphism group  $\text{Aut}_\phi(\overline{F})$  and a field of definition  $E/F$ ; that is,  $\text{Aut}_\phi(E) = \text{Aut}_\phi(\overline{F})$ . This algorithm requires constructing the splitting field of a polynomial with degree  $O(d)$ , so this is not very practical over number fields unless  $d$  is small. Over finite fields it is much more efficient because the average size of the splitting field of a polynomial of degree  $O(d)$  is significantly smaller.

For  $s \in \text{PGL}_2(F)$ , write  $\text{Fix}(s)$  for the set of fixed points of  $s$  in  $\mathbb{P}^1(\overline{F})$ . If  $s$  is an automorphism of  $\phi$ , the action of  $\phi$  on  $\text{Fix}(s)$  is highly restricted, both geometrically and arithmetically. Our second algorithm takes advantage of this fact to compute  $\text{Aut}_\phi(F)$  when  $F$  is any field of characteristic 0 or when  $F$  is a finite field. If  $F$  has characteristic  $p > 0$  and is not finite, then the algorithm only detects the elements of  $\text{Aut}_\phi(F)$  whose order is prime to the characteristic. This algorithm requires finding linear and quadratic factors of a polynomial of degree  $d^2 + 1$ . With the present implementations of root finding and polynomial factoring over number fields available in Sage and Magma, this is infeasible when  $d$  is large. However, the algorithm is quite efficient when  $F$  is a finite field and for number fields when  $d$  is reasonable, say  $d < 15$ .

Our third algorithm computes  $\text{Aut}_\phi(F)$  when  $F$  is a number field. For rational maps of degree at least 15 it is significantly faster than the second method. The main idea here is to first reduce the coefficients modulo  $v$  for several finite places  $v$  of good reduction and compute the automorphism group over the residue field (using our second algorithm). We then use the Chinese remainder theorem to piece together the various automorphisms modulo  $v$  to arrive at the set of automorphisms over the original number field  $F$ .

We first prove a general result about the algebro-geometric structure of  $\text{Aut}_\phi$ . As we will work with automorphism groups over global fields and the reductions at several primes, this type of result is necessary to ensure we are on solid footing. For notation, let  $R$  be a noetherian commutative ring with unity, and let  $R\text{-Alg}$  and  $\mathbf{Grp}$  denote the categories of commutative  $R$ -algebras and groups, respectively. For any  $R$ -algebra  $S$ , we identify  $\text{PGL}_2(S)$  with  $\text{Aut}(\mathbb{P}_S^1)$ , the group of automorphisms of  $\mathbb{P}^1$  defined over  $S$ . We make the following definition:

**Definition.** Let  $\phi : \mathbb{P}_R^1 \rightarrow \mathbb{P}_R^1$  be a nonconstant morphism. The **automorphism group** of  $\phi$  is the  $R$ -group scheme  $\text{Aut}_\phi$  represented by the functor  $\underline{\text{Aut}}_\phi : R\text{-Alg} \rightarrow \mathbf{Grp}$  defined by

$$\underline{\text{Aut}}_\phi(S) = \{f \in \text{Aut}(\mathbb{P}_S^1) : \phi = \phi^f := f \circ \phi \circ f^{-1}\}.$$

**Theorem 1.1.** *Let  $R$  be a commutative ring and let  $\phi : \mathbb{P}_R^1 \rightarrow \mathbb{P}_R^1$  be a nonconstant endomorphism. Then the functor  $\underline{\text{Aut}}_\phi$  is represented by a closed  $R$ -subgroup scheme  $\text{Aut}_\phi \subset \text{PGL}_2$ . If moreover  $\deg(\phi) \geq 2$ , then  $\text{Aut}_\phi$  is finite over  $\text{Spec } R$ .*

*Remark 1.2.* The group scheme  $\text{Aut}_\phi$  need not be flat over  $\text{Spec } R$ . For example, if  $\phi(z) = z^2$  as an endomorphism of  $\mathbb{P}_{\mathbb{Z}}^1$ , then one can check that  $\text{Aut}_\phi(\mathbb{Q}) =$

$\{z, 1/z\} = \text{Aut}_\phi(\overline{\mathbb{F}}_p)$  for  $p > 2$ . But  $\text{Aut}_\phi(\overline{\mathbb{F}}_2) \cong \text{PGL}_2(\mathbb{F}_2)$ , which has order 6. Since the order of a finite flat group scheme is locally constant, we conclude that  $\text{Aut}_\phi$  is not flat over  $\text{Spec } \mathbb{Z}$ .

*Remark 1.3.* If  $\deg(\phi) = 1$ , then  $\text{Aut}_\phi$  is not a finite group scheme in general. Consider the examples  $\phi(z) = z$  and  $\psi(z) = z + 1$ , for which  $\text{Aut}_\phi = \text{PGL}_2$  and  $\text{Aut}_\psi \cong \mathbb{G}_a$ , respectively.

The next result will have two uses in this paper. First, it will allow us to deduce that  $\text{Aut}_\phi$  is proper when  $\phi$  has degree at least 2. Second, it will provide the main tool for relating the automorphism group of an endomorphism over a number field to the automorphism group over a finite field. For the statement, if  $k$  is a non-Archimedean field (not necessarily complete) with valuation ring  $\mathfrak{o}$ , we say that an endomorphism  $\phi : \mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$  has **good reduction** if there exists a morphism  $\Phi : \mathbb{P}_{\mathfrak{o}}^1 \rightarrow \mathbb{P}_{\mathfrak{o}}^1$  with generic fiber  $\phi$ .

**Reduction Lemma.** *Let  $k$  be a non-Archimedean field with valuation ring  $\mathfrak{o}$  and residue field  $\mathbb{F}$ , and let  $\phi \in k(z)$  be a rational function of degree at least 2 (which is equivalent to a morphism  $\mathbb{P}_k^1 \rightarrow \mathbb{P}_k^1$ ). Suppose that  $\phi$  has good reduction. Then every element of  $\text{Aut}_\phi(k)$  has good reduction, and the canonical reduction  $\mathfrak{o} \rightarrow \mathbb{F}$  induces a homomorphism  $\text{red} : \text{Aut}_\phi(k) \rightarrow \text{Aut}_\phi(\mathbb{F})$ . If  $\mathbb{F}$  has characteristic  $p > 0$  (resp. characteristic zero), then the kernel of reduction is a  $p$ -group (resp. trivial).*

If  $K$  is a number field and  $v$  is a finite place of  $K$ , we write  $K_v, \mathbb{Z}_v$ , and  $\mathbb{F}_v$  for the completion of  $K$  at  $v$ , the valuation ring of  $K_v$ , and the residue field of  $K_v$ , respectively. If  $\phi \in K(z)$  is a rational function, we say that it has **good reduction** at  $v$  if all of its coefficients are integral at  $v$ , and it extends to a morphism over  $\text{Spec } \mathbb{Z}_v$ . (Equivalently,  $\phi$  has good reduction if one can reduce its coefficients modulo  $v$ , and the resulting morphism of  $\mathbb{P}_{\mathbb{F}_v}^1$  has the same degree as  $\phi$ .)

**Proposition 1.4.** *Let  $K$  be a number field and let  $\phi \in K(z)$  a rational function of degree  $d \geq 2$ . Define  $S_0$  to be the set of rational primes given by*

$$S_0 = \{2\} \cup \left\{ p \text{ odd} : \frac{p-1}{2} \mid [K : \mathbb{Q}] \text{ and } p \mid d(d^2 - 1) \right\},$$

*and let  $S$  be the (finite) set of places of  $K$  of bad reduction for  $\phi$  along with the places that divide a prime in  $S_0$ . Then  $\text{red}_v : \text{Aut}_\phi(K) \rightarrow \text{Aut}_\phi(\mathbb{F}_v)$  is a well-defined injective homomorphism for all places  $v$  outside  $S$ .*

*Remark 1.5.* In practice, Proposition 1.4 allows one to determine the group structure of  $\text{Aut}_\phi(K)$  very quickly by computing  $\text{Aut}_\phi(\mathbb{F}_v)$  for a few places  $v \notin S$ . This is analogous to the way one typically computes the torsion subgroup of an elliptic curve over a number field; see [16, VII.3]. If one wishes to compute the *elements* of  $\text{Aut}_\phi(K)$  rather than just the group structure, then more work is required.

**Outline.** Section 2 is occupied by the proof of the Reduction Lemma and its corollary. The argument uses techniques from the ramification theory of endomorphisms of the Berkovich projective line; the reader may safely skip the proof and use the Reduction Lemma as a black box if necessary. The proof of Theorem 1.1 is given in Section 3. Section 4 is occupied by the algorithms for computing automorphism groups. Section 5 contains a few examples of our implementation of the algorithms. All of the computations were carried out using Sage [17]. Our code is included with the arXiv distribution of this article. Finally, Section 6 contains a brief discussion

of the scheme  $\text{Conj}_{\phi,\psi}$  of elements of  $\text{PGL}_2$  that conjugate  $\phi$  to  $\psi$ , and we also sketch the main ideas of an algorithm for determining if two endomorphisms  $\phi$  and  $\psi$  are conjugate, i.e., if the scheme  $\text{Conj}_{\phi,\psi}$  has any points.

## ACKNOWLEDGEMENTS

This project began at the University of Georgia, during an NSF-sponsored summer school on Arithmetic Dynamics. We thank the organizer, Robert Rumely, for the experience. The authors are grateful for the opportunity to complete the project at the Institute for Computational and Experimental Research in Mathematics. Finally, we would like to thank Joseph H. Silverman for helpful comments on our number field algorithm.

## 2. PROOF OF THE REDUCTION LEMMA

For background on the Berkovich projective line and dynamics, see [3]. For a more concise summary of the necessary ideas, we direct the reader to [6].

Let  $\mathbb{C}_k$  be the completion of an algebraic closure of the completion of  $k$ , and let  $\mathbf{P}^1$  be the Berkovich analytification of the projective line  $\mathbb{P}_{\mathbb{C}_k}^1$ . The morphism  $\phi$  extends functorially to  $\mathbf{P}^1$ . We use two key facts due to Rivera-Letelier [14, Thm. 4]: (1)  $\phi$  has good reduction if and only if the Gauss point  $\zeta \in \mathbf{P}^1$  is totally invariant, and (2) a rational function has at most one totally invariant point in  $\mathbf{P}^1 \setminus \mathbb{P}^1(\mathbb{C}_k)$ .

For  $f \in \text{Aut}_{\phi}(k)$ , we have

$$f^{-1}(\zeta) = f^{-1}(\phi^{-1}(\zeta)) = (\phi \circ f)^{-1}(\zeta) = (f \circ \phi)^{-1}(\zeta) = \phi^{-1}(f^{-1}(\zeta)).$$

Hence  $f^{-1}(\zeta)$  is a totally invariant type II point for  $\phi$ , so that  $f(\zeta) = \zeta$ . Equivalently,  $f$  has good reduction. Thus the reduction map  $\text{red} : \text{Aut}_{\phi}(k) \rightarrow \text{Aut}_{\phi}(\mathbb{F})$  is well-defined, and it is evidently a homomorphism.

Now we compute the kernel of reduction. Suppose  $\text{red}(f)$  is trivial. Without loss of generality, we may replace  $k$  with a finite extension in order to assume that  $f$  has a  $k$ -rational fixed point. Moreover, we may conjugate  $f$  by an element of  $\text{PGL}_2(\mathfrak{o})$  in order to assume that  $f(\infty) = \infty$ . Now  $f(z) = \alpha z + \beta$ . If  $f$  has order  $m > 1$ , then the equation  $f^m(z) = f(z)$  shows that  $\alpha$  is an  $m$ -th root of unity. But  $\text{red}(f)$  is trivial, so we have  $\tilde{\alpha} = 1$ . If  $k$  has residue characteristic zero, then we conclude that  $\alpha = 1$  and  $\beta = 0$ . Otherwise, we find that  $\alpha$  is a  $p$ -power root of unity in  $k$ , and hence  $f$  has  $p$ -power order in  $\text{Aut}_{\phi}(k)$ . The proof of the Reduction Lemma is complete.

*Remark 2.1.* A different proof of the first part of the Reduction Lemma can be given using the maximum modulus principle in non-Archimedean analysis [12, Lem. 6].

**Proposition 2.2.** *Let  $F$  be a field, and let  $n \geq 2$  be an integer. Suppose that  $\phi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$  is a morphism of degree  $d \geq 2$  such that  $\text{Aut}_{\phi}(F)$  contains an element of order  $n$ . Then  $n$  divides  $d(d^2 - 1)$ .*

*Proof.* We may assume without loss of generality that  $F$  is algebraically closed. Let  $s \in \text{Aut}_{\phi}(F)$  have order  $n$ . We conjugate one of the fixed points of  $s$  to  $\infty$ , so that  $s = \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix}$ . (Note that replacing  $s$  with  $usu^{-1}$  has the effect of replacing  $\phi$  with  $u \circ \phi \circ u^{-1}$ .) The proof divides into two cases, depending on whether  $s$  has one or two fixed points.

If  $s$  has only one fixed point, then necessarily  $n = \text{char}(F)$  is prime and  $\alpha = 1$ . (See, for example, [5, Lem. 3.1].) Replace  $s$  with  $\begin{pmatrix} \beta^{-1} & \\ & 1 \end{pmatrix} s \begin{pmatrix} \beta & \\ & 1 \end{pmatrix}$  in order to assume that  $\beta = 1$ . It follows that  $\phi(z+1) - 1 = \phi(z)$ , or equivalently, that the function  $\phi(z) - z$  is invariant under the map  $z \mapsto z+1$ . Hence there exists a rational function  $\psi(z) \in F(z)$  such that  $\phi(z) - z = \psi(z^n - z)$ . We conclude that  $\deg(\phi) = n \cdot \deg(\psi)$  or  $n \cdot \deg(\psi) + 1$ .

Now suppose that  $s$  has two distinct fixed points:  $\infty$  and  $\beta/(1-\alpha)$ . We may conjugate the second fixed point to 0 in order to assume that  $\beta = 0$ . Note that this implies that  $\alpha \in F^\times$  has multiplicative order  $n$ . To say that  $s$  is an automorphism of  $\phi$  is equivalent to saying that  $\phi(z)/z$  is invariant under the map  $z \mapsto \alpha z$ . Hence there is a rational function  $\psi \in F(z)$  such that  $\phi(z)/z = \psi(z^n)$ . So  $\deg(\phi) = n \cdot \deg(\psi)$  or  $n \cdot \deg(\psi) \pm 1$ .  $\square$

*Proof of Proposition 1.4.* By the Reduction Lemma, it suffices to prove that if  $v \notin S$ , then  $\text{Aut}_\phi(K)$  has no element of order  $p$ , where  $v \mid p$ . Suppose otherwise.

The group  $\text{PGL}_2(K)$  contains an element of order  $p$  if and only if  $\zeta_p + \zeta_p^{-1} \in K$  for some primitive  $p$ -th root of unity  $\zeta_p$  [4]. Note that  $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{1}{2}(p-1)$  for  $p > 2$ , so that  $\frac{p-1}{2} \mid [K : \mathbb{Q}]$ . If  $\text{Aut}_\phi(K)$  contains an element of order  $p$ , then  $p$  divides  $d(d^2 - 1)$  by Proposition 2.2. Hence  $p \in S_0$ , and so  $v \in S$ .  $\square$

### 3. PROOF OF THEOREM 1.1

Fix a commutative ring  $R$ . Over  $R$ ,  $\text{PGL}_2$  may be embedded as an affine subvariety of  $\mathbb{P}_R^3 = \text{Proj } R[a, b, c, d]$ ; indeed, it is the complement of the quadric  $ad - bc = 0$ . Let  $\phi : \mathbb{P}_R^1 \rightarrow \mathbb{P}_R^1$  be a nonconstant endomorphism. We may define  $\text{Aut}_\phi$  as a subgroup scheme of  $\text{PGL}_2$  as follows. After fixing coordinates of  $\mathbb{P}_R^1$ , the morphism  $\phi$  can be given by a pair of homogeneous polynomials  $\Phi = (\Phi_0(X, Y), \Phi_1(X, Y))$  of degree  $D = \deg(\phi)$  with coefficients in  $R$  such that the homogeneous resultant  $\text{Res}(\Phi_0, \Phi_1)$  is a unit in  $R$ . The pair  $\Phi_0, \Phi_1$  is unique up to multiplication by a common unit in  $R$ . Similarly, for any  $R$ -algebra  $S$ , an element  $f \in \text{PGL}_2(S)$  may be given by a pair  $F = (aX + bY, cX + dY)$  with  $a, b, c, d \in S$  and  $ad - bc \in S^\times$ . Note that  $f^{-1}$  is represented by the pair  $F^{-1} := (dX - bY, -cX + aY)$ . Then  $f \circ \phi \circ f^{-1} = \phi$  is equivalent to saying that  $F \circ \Phi \circ F^{-1}$  and  $\Phi$  define the same morphism on  $\mathbb{P}_S^1 \rightarrow \mathbb{P}_S^1$ . If  $F \circ \Phi \circ F^{-1} = (\Psi_0(X, Y), \Psi_1(X, Y))$ , then this means

$$\Phi_0(X, Y)\Psi_1(X, Y) - \Phi_1(X, Y)\Psi_0(X, Y) = 0. \quad (3.1)$$

The expression on the left is a homogeneous polynomial of degree  $2D$  in  $X$  and  $Y$  whose coefficients are homogeneous polynomials in  $R[a, b, c, d]$ . So (3.1) gives  $2D + 1$  equations that cut out a closed subscheme of  $\text{PGL}_2$  defined over  $R$ . One checks readily that  $\text{Aut}_\phi(S)$  is a subgroup of  $\text{PGL}_2(S)$  for every  $S$ .

Next we argue that  $\text{Aut}_\phi$  is a finite group scheme over  $R$  when  $\phi$  has degree at least 2. The map  $\text{Aut}_\phi \rightarrow \text{Spec } R$  is quasi-finite. Indeed, it suffices to check this statement on geometric fibers, and Silverman has shown that  $\text{Aut}_\phi(L)$  is a finite group for any algebraically closed field  $L$  [15, Prop. 4.65].<sup>1</sup>

Moreover,  $\text{Aut}_\phi$  is proper over  $\text{Spec } R$ . Indeed, since  $\text{Aut}_\phi$  and  $\text{Spec } R$  are noetherian, this can be checked using the valuative criterion for properness using only

<sup>1</sup>Alternatively, §4.1 gives a slightly simpler proof of Silverman's result.

discrete valuation rings [8, Ex. II.4.11]. Let  $\mathfrak{o}$  be a discrete valuation ring with field of fractions  $k$ , and consider a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec} k & \longrightarrow & \mathrm{Aut}_\phi \\ \downarrow & \nearrow & \downarrow \\ \mathrm{Spec} \mathfrak{o} & \longrightarrow & \mathrm{Spec} R. \end{array}$$

The left vertical map is the canonical open immersion, and the right vertical map is the structure morphism. We must show there is a unique morphism  $\mathrm{Spec} \mathfrak{o} \rightarrow \mathrm{Aut}_\phi$  that makes the entire diagram commute. Without loss of generality, we may assume that  $R = \mathfrak{o}$  and that the lower horizontal arrow is the identity map.

If  $v : k \rightarrow \mathbb{Z} \cup \{+\infty\}$  is the canonical extension of the valuation on  $\mathfrak{o}$ , then we may endow  $k$  with the structure of a non-Archimedean field by setting  $|x| = e^{-v(x)}$  for every  $x \in k$ . (Note that we interpret  $e^{-\infty}$  as zero.) Since  $\phi$  is defined over  $\mathfrak{o}$ , it has good reduction. The Reduction Lemma asserts that every  $k$ -automorphism of  $\phi$  also has good reduction. Equivalently, every  $k$ -valued point may be extended to an  $\mathfrak{o}$ -valued point, which is what we wanted to show.

We now know that  $\mathrm{Aut}_\phi \rightarrow \mathrm{Spec} R$  is a quasi-finite proper morphism. Zariski's main theorem tells us that it factors as an open immersion of  $R$ -schemes  $\mathrm{Aut}_\phi \rightarrow X$  followed by a finite morphism  $X \rightarrow \mathrm{Spec} R$ . But  $\mathrm{Aut}_\phi$  is proper, so any open immersion is actually an isomorphism. Hence  $\mathrm{Aut}_\phi$  is finite over  $\mathrm{Spec} R$ . This completes the proof of Theorem 1.1.

#### 4. ALGORITHMS

**4.1. Absolute Automorphism Groups — Method of Invariant Sets.** Let  $F$  be an arbitrary field, and suppose  $\phi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$  is a morphism of degree at least 2. In this section we describe an algorithm to compute  $\mathrm{Aut}_\phi(\overline{F})$ , where  $\overline{F}$  is an algebraic closure of  $F$ . In fact, we will see that it also gives a field of definition  $E/F$  for the absolute automorphism group, although  $E$  is typically not the smallest such field. The idea is to use a finite  $\mathrm{Aut}_\phi(\overline{F})$ -invariant subset of  $\mathbb{P}^1(\overline{F})$  to produce a set of candidate automorphisms, and then to sort through the candidates by brute force. We begin by explaining Algorithm 1, which determines the automorphism group if we already have such an invariant set  $T$ . Then we give a description of how one constructs  $T$ .

Suppose that we are given a finite set  $T = \{\tau_1, \dots, \tau_n\} \subset \mathbb{P}^1(\overline{F})$  with  $n \geq 3$  on which  $\mathrm{Aut}_\phi(\overline{F})$  acts. Let  $E = F(\tau_1, \dots, \tau_n)$  be the field of definition for  $T$ . Let  $s \in \mathrm{Aut}_\phi(E)$ . Since we assume  $T$  is invariant, there must be a triple of distinct indices  $i, j, k \in \{1, \dots, n\}$  such that  $s(\tau_1) = \tau_i$ ,  $s(\tau_2) = \tau_j$ , and  $s(\tau_3) = \tau_k$ .

Conversely, given a triple of distinct indices  $i, j, k \in \{1, \dots, n\}$ , there exists a unique element  $s \in \mathrm{PGL}_2(E)$  such that  $s(\tau_1) = \tau_i$ ,  $s(\tau_2) = \tau_j$ , and  $s(\tau_3) = \tau_k$ . One now determines if this candidate element  $s$  actually satisfies the functional equation  $s \circ \phi = \phi \circ s$ ; if that is the case, then  $s \in \mathrm{Aut}_\phi(E)$ . See Algorithm 1.

A natural candidate for an  $\mathrm{Aut}_\phi(\overline{F})$ -invariant set is the set of fixed points of  $\phi$ . For let  $x \in \mathbb{P}^1(\overline{F})$  be a fixed point, and let  $s \in \mathrm{Aut}_\phi(\overline{F})$ . Then

$$s(x) = s(\phi(x)) = \phi(s(x)), \quad (4.1)$$

---

**Algorithm 1** — Compute  $\text{Aut}_\phi(E)$  given an  $\text{Aut}_\phi(\overline{E})$ -invariant subset of  $\mathbb{P}^1(E)$  consisting of  $n \geq 3$  points

---

Input:

- a nonconstant rational function  $\phi \in E(z)$
- an  $\text{Aut}_\phi(\overline{E})$ -invariant subset  $T = \{\tau_1, \dots, \tau_n\} \subset \mathbb{P}^1(E)$ ,  $n \geq 3$

Output: the set  $\text{Aut}_\phi(E)$

create an empty list  $L$

for each triple of distinct integers  $i, j, k \in \{1, \dots, n\}$ :

    compute  $s \in \text{PGL}_2(E)$  by solving the linear system

$$s(\tau_1) = \tau_i, \quad s(\tau_2) = \tau_j, \quad s(\tau_3) = \tau_k$$

    if  $s \circ \phi = \phi \circ s$ : append  $s$  to  $L$

return  $L$

---

which shows that  $s(x)$  is also a fixed point. A general rational function  $\phi$  of degree  $d \geq 2$  has  $d + 1 \geq 3$  distinct fixed points. Thus the choice  $T = \text{Fix}(\phi)$  will suffice in most circumstances.

If instead  $\text{Fix}(\phi)$  has cardinality 2, define  $T = \phi^{-1}(\text{Fix}(\phi))$ . This set is  $\text{Aut}_\phi(\overline{F})$ -invariant: if  $x \in \text{Fix}(\phi)$ ,  $y \in \phi^{-1}(x)$ , and  $s \in \text{Aut}_\phi(\overline{F})$ , then

$$\phi(s(y)) = s(\phi(y)) = s(x).$$

Since  $s(x)$  is a fixed point by equation (4.1), we find  $s(y) \in \phi^{-1}(\text{Fix}(\phi))$ . Recall that we require  $\#T \geq 3$ , and by construction we have  $\#T \geq 2$  since  $\text{Fix}(\phi) \subseteq T$ . If  $\#T = 2$ , then  $T = \text{Fix}(\phi)$ , and each of the fixed points is totally ramified for  $\phi$ . This implies that the derivative at each of the fixed points vanishes,<sup>2</sup> which in turn means each element of  $\text{Fix}(\phi)$  has fixed point multiplicity 1. But the total number of fixed points of a map of degree  $d$  is  $d + 1 \geq 3$ , counting multiplicities, so we have a contradiction. (See, for example, [7, Appx. A].)

Finally, suppose that  $\text{Fix}(\phi) = \{x\}$ . We claim that  $\#\phi^{-1}(x) \geq 2$ . For otherwise  $x$  is ramified for  $\phi$ , which implies that the derivative  $\phi'(x)$  vanishes there. But the fact that  $x$  is the unique fixed point of  $\phi$  means that in local coordinates centered at  $x$  our map is of the form  $z \mapsto z + a_{d+1}z^{d+1} + \dots$  with  $a_{d+1} \neq 0$ . So the derivative cannot vanish at  $x$ , and we must have  $\#\phi^{-1}(x) \geq 2$  as desired. If  $\#\phi^{-1}(x) \geq 3$ , then set  $T = \phi^{-1}(x)$ . Otherwise,  $\phi^{-1}(x) = \{x, y\}$ ; set  $T = \phi^{-2}(x) = \{x, y\} \cup \phi^{-1}(y)$ , which satisfies  $3 \leq \#T \leq d + 2$ . The argument in the preceding paragraph shows that  $T$  is  $\text{Aut}_\phi(\overline{F})$ -invariant in all cases.

Algorithm 2 gives the complete description of this method for computing the automorphism group of a rational function defined over an arbitrary field  $F$ .

**4.2. Method of Fixed Points.** Let  $F$  be a finite field or a field of characteristic zero, and let  $\phi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$  a nonconstant morphism. For any  $\phi$ -periodic point  $x \in \mathbb{P}^1(\overline{F})$ , write  $\text{per}(x)$  for its exact period — i.e., the minimum positive integer  $i$  such that  $\phi^i(x) = x$ . If  $x$  is not periodic, write  $\text{per}(x) = +\infty$ . For each pair of integers  $i, j \in \{1, 2\}$ , define the following set:

$$Z_{i,j} = \{x \in \mathbb{P}^1(\overline{F}) : \text{per}(x) = i, [F(x) : F] = j\}. \quad (4.2)$$

---

<sup>2</sup>More precisely, the induced map  $T\phi$  on the tangent space  $T\mathbb{P}_x^1$  is zero.



---

**Algorithm 2** — Computation of  $\text{Aut}_\phi(\overline{F})$  via the method of invariant sets

---

Input: a field  $F$  and a rational function  $\phi \in F(z)$  of degree at least 2

Output: a field extension  $E/F$  and the set  $\text{Aut}_\phi(E) = \text{Aut}_\phi(\overline{F})$

if  $\#\text{Fix}(\phi) \geq 3$ :

    compute  $\text{Aut}_\phi(E)$  using Algorithm 1 with  $T = \text{Fix}(\phi)$  and  $E = F(T)$

else if  $\#\text{Fix}(\phi) = 2$ :

    compute  $\text{Aut}_\phi(E)$  using Algorithm 1 with  $T = \phi^{-1}(\text{Fix}(\phi))$  and  $E = F(T)$

else:

    compute  $\text{Aut}_\phi(E)$  using Algorithm 1 with  $T = \phi^{-2}(\text{Fix}(\phi))$  and  $E = F(T)$

return  $E$  and  $\text{Aut}_\phi(E)$

---

We also define the following set of ordered pairs:

$$W = \{(x, y) : x \in Z_{1,1}, y \in \phi^{-1}(x), [F(y) : F] = 1\}. \quad (4.3)$$

(More concretely,  $W$  is the set of pairs of  $F$ -rational points such that  $x$  is fixed by  $\phi$  and  $\phi(y) = x$ .) These sets may be constructed by factoring the polynomials that define the fixed points of  $\phi$ , the points of period 2, and the preimages of  $F$ -rational points. We write  $Z^{(2)}$  for the set of unordered pairs of elements of a set  $Z$ .

Suppose that  $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{Aut}_\phi(F)$  is nontrivial. The homogeneous polynomial defining the fixed points of  $s$  is  $\gamma X^2 + (\delta - \alpha)XY - \beta Y^2$ . If  $s$  has a unique fixed point  $x$ , then  $F$  is a field of characteristic  $p > 0$ . (To see this, move the unique fixed point to infinity. Then  $s$  is a translation with finite order.) So we conclude that  $F = \mathbb{F}_q$ , that  $x$  is  $F$ -rational (because  $F$  is perfect), and that  $s$  has order  $p$  [5, Lem. 3.1]. Now

$$s(\phi(x)) = \phi(s(x)) = \phi(x), \text{ so that } \phi(x) = x.$$

Hence  $x \in Z_{1,1}$ . Choose  $u \in \text{PGL}_2(F)$  such that  $u(x) = \infty$ ; then  $usu^{-1} = \begin{pmatrix} 1 & \lambda \\ & 1 \end{pmatrix}$  for some  $\lambda \in F \setminus \{0\}$ . That is,  $s \in u^{-1} \begin{pmatrix} 1 & F \setminus \{0\} \\ & 1 \end{pmatrix} u$ . In order to find all elements of  $\text{Aut}_\phi(F)$  of order  $p$ , it suffices to apply this technique to every  $x$  in the set  $Z_{1,1}$ . See the first for-loop of Algorithm 3.

Now suppose that  $s \in \text{Aut}_\phi(F)$  has precisely two distinct fixed points  $x_1$  and  $x_2$ . Then  $s(\phi(x_1)) = \phi(s(x_1)) = \phi(x_1)$ , so that  $\phi(x_1) \in \{x_1, x_2\}$ . There are three possible cases: (1)  $\phi$  fixes both  $x_1$  and  $x_2$ ; (2)  $\phi$  swaps  $x_1$  and  $x_2$ ; or (3)  $\phi(x_1) = x_2$  and  $\phi$  fixes  $x_2$  (perhaps after interchanging  $x_1$  and  $x_2$ ). Since  $\phi$  is defined over  $F$ , all Galois conjugates of a fixed point must also be fixed points. Thus in cases (1) and (2), either  $x_1$  and  $x_2$  are both  $F$ -rational, or they are quadratic conjugates over  $F$ . In case (3), both  $x_1$  and  $x_2$  must be  $F$ -rational.

If  $x_1$  and  $x_2$  are both  $F$ -rational in case (1) — so that  $(x_1, x_2) \in Z_{1,1}^{(2)}$  — then we may select  $u \in \text{PGL}_2(F)$  such that  $u(x_1) = \infty$  and  $u(x_2) = 0$ . Then  $usu^{-1} = \begin{pmatrix} \zeta & \\ & 1 \end{pmatrix}$  for some root of unity  $\zeta \in F$ . If  $\zeta$  has order  $n$ , then  $n \mid d(d^2 - 1)$  by Proposition 2.2. Let  $T$  be the set of roots of unity in  $F$  that have order dividing  $d(d^2 - 1)$ . We loop over all distinct unordered pairs of elements  $(x_1, x_2) \in Z_{1,1}^{(2)}$ , and check which elements of  $u^{-1} \begin{pmatrix} T & \\ & 1 \end{pmatrix} u$  lie in  $\text{Aut}_\phi(F)$ . See the second for-loop of Algorithm 3. In fact, this strategy works in case (2) when  $x_1, x_2$  are both  $F$ -rational, and in case (3). These correspond to looping over pairs  $(x_1, x_2)$  in  $Z_{2,1}^{(2)}$  and in  $W$ , respectively.



Now suppose  $x_1$  and  $x_2$  are quadratic Galois conjugates over  $F$  in case (1), so that  $(x_1, x_2) \in Z_{1,2}^{(2)}$ . Then  $E = F(x_1, x_2)$  is a quadratic extension. In this case, we may choose  $u \in \text{PGL}_2(E)$  satisfying  $u(x_1) = \infty$  and  $u(x_2) = 0$ , so that  $usu^{-1} = \begin{pmatrix} \xi & \\ & 1 \end{pmatrix}$  for some root of unity  $\xi \in E$ . In particular, if the fixed points of  $s$  are  $a \pm b\sqrt{d}$ , we may take

$$u = \begin{pmatrix} 1 & -a - b\sqrt{d} \\ 1 & -a + b\sqrt{d} \end{pmatrix}, \text{ so } s = u^{-1} \begin{pmatrix} \xi & \\ & 1 \end{pmatrix} u = \begin{pmatrix} a + \frac{(1+\xi)b\sqrt{d}}{(1-\xi)} & -a^2 + b^2d \\ 1 & -a + \frac{(1+\xi)b\sqrt{d}}{(1-\xi)} \end{pmatrix}.$$

Let  $\sigma$  be the nontrivial element of  $\text{Gal}(E/F)$ . Since  $s \in \text{PGL}_2(F)$ , we have

$$\sigma \left( \frac{(1+\xi)b\sqrt{d}}{(1-\xi)} \right) = \frac{-(1+\xi^\sigma)b\sqrt{d}}{(1-\xi^\sigma)} = \frac{(1+\xi)b\sqrt{d}}{(1-\xi)},$$

which implies that  $\xi^\sigma \xi = 1$ . If  $\sigma$  acts trivially on  $\xi$ , we must have  $\xi = -1$  (since  $s$  is nontrivial). Otherwise,  $E = F(\xi)$ . In particular,  $F(x_1, x_2)$  is always a cyclotomic extension of  $F$ .

If  $F = \mathbb{F}_q$  is a finite field, then  $\xi \in \mathbb{F}_{q^2}$ . Since the automorphism  $\sigma$  acts by Frobenius on  $\mathbb{F}_{q^2}$ , it follows that  $\xi^\sigma \xi = \xi^{q+1} = 1$ . That is, a nontrivial element of  $\text{PGL}_2(\mathbb{F}_q)$  with two quadratic conjugate fixed points necessarily has order dividing  $q+1$ . In this case, let  $\Lambda \subset \mathbb{F}_{q^2}^\times$  be the unique subgroup of order  $q+1$ ; note that  $\Lambda$  always contains  $-1$ .

If  $F$  is a field of characteristic zero, let  $C(X) = X^{d(d^2-1)} - 1$ . In this case, let  $\Lambda$  be the set of roots of the quadratic factors of  $C(X)$  over  $F$  together with  $-1$ .

To detect  $s$ , loop over all Galois conjugate pairs in  $Z_{1,2}^{(2)}$  and check which elements of  $u^{-1} \begin{pmatrix} \Lambda & \\ & 1 \end{pmatrix} u$  lie in  $\text{Aut}_\phi(F)$ . See the third for-loop of Algorithm 3. The same strategy also applies if we are in case (2) and  $x_1$  and  $x_2$  are quadratic conjugates.

*Remark 4.1.* The first for-loop in Algorithm 3 will not terminate if  $F$  is an infinite field of characteristic  $p$ . But the remainder of the algorithm proceeds without modification and computes  $\{s \in \text{Aut}_\phi(F) : \gcd(\text{order of } s, \text{char}(F)) = 1\}$ .

*Remark 4.2.* When  $F$  is a number field, the technique in the proof of Proposition 1.4 gives further restrictions on the set of roots of unity one must include in the set  $\Lambda$ . It suffices to consider  $F$ -rational and  $F$ -quadratic roots of  $X^m - 1$ , where  $m$  is the product of all integers  $n$  such that  $\varphi(n) \mid 2[F : \mathbb{Q}]$ . Here  $\varphi$  is Euler's function.

**4.3. Chinese Remainder Theorem Method for Number Fields.** In this section, we assume that our field  $K$  is a number field. As discussed in the previous section, Algorithm 3 computes  $\text{Aut}_\phi(K)$ . This algorithm requires computing the irreducible factors of degree at most 2 of a degree  $d^2 + 1$  polynomial, namely the polynomial obtained by clearing denominators in the equation  $\phi \circ \phi(z) = z$ . As the degree becomes large, this quickly becomes impractical on computer algebra systems, even over  $K = \mathbb{Q}$ . Thus, we have a need for an alternative algorithm over number fields.

We use an approach that is ubiquitous in number theory: first compute the automorphism group over a residue field  $\mathbb{F}_v$  for some finite place(s)  $v$ , and then use the local information to obtain a global answer. More precisely, our method is as follows.

Let  $v = v_0$  be a finite prime such that the reduction map  $\text{Aut}_\phi(K) \rightarrow \text{Aut}_\phi(\mathbb{F}_v)$  is injective, e.g.  $v \notin S$  as defined in Proposition 1.4. Now compute  $\text{Aut}_\phi(\mathbb{F}_v)$  using

**Algorithm 3** — Computation of  $\text{Aut}_\phi(F)$  via the method of fixed points

---

Input: a field  $F$ , finite or of characteristic zero, and  $\phi \in F(z)$  of degree  $\geq 2$ 

Output: the set  $\text{Aut}_\phi(F)$ 

if  $F = \mathbb{F}_q$  is a finite field:

    create a list  $T = \mathbb{F}_q^\times$ 

    create a list  $\Lambda$  of  $\xi \in \mathbb{F}_{q^2}^\times \setminus \{1\}$  with  $\xi^{q+1} = 1$ 

else:

    let  $C(X) = X^{d(d^2-1)} - 1$ 

    create a list  $T$  of  $F$ -rational roots of  $C(X)$ 

    create a list  $\Lambda$  of roots of  $F$ -quadratic factors of  $C(X)$  and  $-1$ 

create a list  $L = [z]$ 

create the sets  $Z_{i,j}, W$  defined in equations (4.2) and (4.3)

for  $x \in Z_{1,1}$ :

    choose  $u \in \text{PGL}_2(F)$  such that  $u(x) = \infty$ 

    for  $\lambda \in T$ :

        set  $s(z) = u^{-1}(u(z) + \lambda)$ 

        if  $s \circ \phi = \phi \circ s$ : append  $s$  to  $L$ 

for each pair  $(x, y)$  with  $x \neq y$  in  $Z_{1,1}^{(2)} \cup Z_{2,1}^{(2)} \cup W$ :

    choose  $u \in \text{PGL}_2(F)$  such that  $u(x) = \infty$  and  $u(y) = 0$ 

    for  $\zeta \in T \setminus \{1\}$ :

        set  $s(z) = u^{-1}(\zeta u(z))$ 

        if  $s \circ \phi = \phi \circ s$ : append  $s$  to  $L$ 

for each pair of Galois conjugates  $(x, y)$  in  $Z_{2,1}^{(2)} \cup Z_{2,2}^{(2)}$ :

    choose  $u \in \text{PGL}_2(F(x, y))$  such that  $u(x) = \infty$  and  $u(y) = 0$ 

    for  $\xi \in \Lambda$ :

        set  $s(z) = u^{-1}(\xi u(z))$ 

        if  $s \circ \phi = \phi \circ s$ : append  $s$  to  $L$ 

return  $L$ 


---

Algorithm 3. For each element in  $\text{Aut}_\phi(\mathbb{F}_v)$ , let  $f \in \text{Aut}(\mathbb{P}_K^1)$  be a lift of minimal height and check if  $f \in \text{Aut}_\phi(K)$ . If every element of  $\text{Aut}_\phi(\mathbb{F}_v)$  lifts to an element of  $\text{Aut}_\phi(K)$ , then we are done. Otherwise, we will repeat this process, with some minor modifications; we explain these modifications now.

Let  $v_1$  be finite prime outside of  $S \cup \{v_0\}$  and compute  $\text{Aut}_\phi(\mathbb{F}_{v_1})$ . Let  $G \subseteq \text{Aut}(\mathbb{P}_{\mathcal{O}_K/\prod v_i}^1)$  be a subset that surjects onto  $\text{Aut}_\phi(\mathbb{F}_{v_i})$  for each  $i$ ; this step is called the CRT (Chinese Remainder Theorem) step. For each element of  $G$ , choose a lift  $f \in \text{Aut}(\mathbb{P}_K^1)$  of minimal height. If  $f \circ \phi = \phi \circ f$  then add  $f$  to the list **Auts**. If **Auts** surjects onto  $\text{Aut}_\phi(\mathbb{F}_{v_i})$  for any  $i$ , then we are done. If not, then choose another prime  $v_{i+1} \notin S \cup \{v_0, \dots, v_i\}$  and repeat.

In order to make this method into an algorithm, we need to provide a terminating condition. Write  $N(v)$  for the norm of a finite prime  $v$ . We claim that if  $\prod_i N(v_i) \geq (2M)^{[K:\mathbb{Q}]}$ , for some explicitly computable constant  $M$ , then **Auts** =  $\text{Aut}_\phi(K)$ , even if **Auts** does not surject onto  $\text{Aut}_\phi(\mathbb{F}_{v_i})$  for any  $i$ . We will spend the rest of the section proving this claim via the theory of heights.

Let  $H_K: \mathbb{P}^1(K) \rightarrow \mathbb{R}_{\geq 1}$  denote the relative multiplicative height for  $K$  and let  $L_2(f)$  denote the  $L_2$ -norm of a polynomial  $f$ . See, for example, [9, B.2, B.7] for definitions.

**Proposition 4.3.** *Let  $T, T' \subset \mathbb{P}^1(\overline{K})$  be Galois invariant sets of order at least 3, and let  $f_T, f_{T'} \in K[w, z]_{(0)}$  be square-free polynomials such that  $V(f_T) = T$  and  $V(f_{T'}) = T'$ . Then for any  $s \in \text{Aut}(\mathbb{P}_K^1) \subset \mathbb{P}^3(\overline{K})$  such that  $s(T) = T'$ , we have  $H_K(s) \leq 6^{[K:\mathbb{Q}]} L_2(f_T)^3 L_2(f_{T'})^3$ .*

*Proof.* Let  $s$  be as in the statement of the Proposition. Let  $\tau_1, \tau_2, \tau_3$  be 3 distinct elements of  $T$ , and let  $\eta_i := s(\tau_i) \in T'$ . In coordinates, we write  $\tau_i = (\tau_{i,0} : \tau_{i,1})$  and  $\eta_i = (\eta_{i,0} : \eta_{i,1})$ . Since an automorphism of  $\mathbb{P}^1$  is determined by its action on 3 elements, we have an expression for  $s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  in terms of  $\tau_{i,j}, \eta_{i,j}$ , i.e.

$$\begin{aligned} \alpha &= \sum_{\sigma \in S_3} (\text{sgn } \sigma) B_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}, & \beta &= \sum_{\sigma \in S_3} (\text{sgn } \sigma) A_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}, \\ \gamma &= \sum_{\sigma \in S_3} (\text{sgn } \sigma) A_{\sigma(1)} B_{\sigma(2)} D_{\sigma(3)}, & \delta &= \sum_{\sigma \in S_3} (\text{sgn } \sigma) A_{\sigma(1)} B_{\sigma(2)} C_{\sigma(3)}, \end{aligned}$$

where  $A_i = \tau_{i,0}\eta_{i,1}$ ,  $B_i = -\tau_{i,1}\eta_{i,1}$ ,  $C_i = -\tau_{i,0}\eta_{i,0}$ , and  $D_i = \tau_{i,1}\eta_{i,0}$ .

This expression allows us to obtain a bound on the local height of  $s$ . Let  $v$  be any place of  $K$  and let  $\varepsilon_v = 6$  if  $v \mid \infty$  and  $\varepsilon = 1$  if  $v \nmid \infty$ . Then, by the triangle inequality,

$$|\alpha|_v \leq \varepsilon_v \cdot \max_{\sigma \in S_3} |B_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}|_v \leq \varepsilon_v \prod_{1 \leq i \leq 3} \max\{|\tau_{i0}|_v, |\tau_{i1}|_v\} \cdot \max\{|\eta_{i0}|_v, |\eta_{i1}|_v\}.$$

One can easily check that the same bound holds for  $|\beta|_v, |\gamma|_v, |\delta|_v$ . It follows that

$$\begin{aligned} H_K(s) &= \prod_v \max\{|\alpha|_v, |\beta|_v, |\gamma|_v, |\delta|_v\}^{[K_v:\mathbb{Q}_v]} \\ &\leq \prod_v \varepsilon_v^{[K_v:\mathbb{Q}_v]} \cdot \prod_{1 \leq i \leq 3} \max\{|\tau_{i0}|_v, |\tau_{i1}|_v\}^{[K_v:\mathbb{Q}_v]} \cdot \max\{|\eta_{i0}|_v, |\eta_{i1}|_v\}^{[K_v:\mathbb{Q}_v]} \\ &= 6^{[K:\mathbb{Q}]} \prod_{1 \leq i \leq 3} H_K(\tau_i) H_K(\eta_i). \end{aligned}$$

Since  $H_K(\tau_i) \leq L_2(f_T)$  and  $H_K(\eta_i) \leq L_2(f_{T'})$  [9, Lemma B.7.3.1], this completes the proof.  $\square$

**Corollary 4.4.** *Let  $\phi \in K(z)$  be a rational function of degree  $> 1$ , let  $T \subset \mathbb{P}^1(\overline{K})$  be the Galois invariant set constructed in Algorithm 2 (with  $F = K$ ), and let  $f_T$  be a square-free polynomial such that  $V(f_T) = T$ . Then every element of  $\text{Aut}_\phi(K) \subset \mathbb{P}^3(K)$  has relative multiplicative height bounded by  $6^{[K:\mathbb{Q}]} L_2(f_T)^6$ .*

We will take this height bound  $6^{[K:\mathbb{Q}]} L_2(f_T)^6$  to be our explicit constant  $M$ . Now we need to show that if  $\prod_i N(v_i) \geq (2M)^{2[K:\mathbb{Q}]}$ , then every element of  $\text{Aut}_\phi(K)$  is a lift of an element of  $\prod_i \text{Aut}_\phi(\mathbb{F}_{v_i})$  of minimal height. We will need the following two lemmas.

**Lemma 4.5.** *Let  $\mathfrak{b}$  be a nonzero fractional ideal of  $\mathcal{O}_K$ , and write it as a quotient  $\mathfrak{b} = \mathfrak{b}^+/\mathfrak{b}^-$  of relatively prime integral ideals. Then  $H_K(\beta) \geq N(\mathfrak{b}^+)$  for all nonzero  $\beta \in \mathfrak{b}$ .*

*Proof.* Since  $\beta \in \mathcal{O}_K$ , we have  $|\beta|_v \leq 1$  for any finite place  $v$ . Therefore

$$\begin{aligned} H_K(\beta) &= \prod_{v|\infty} \max\{1, |\beta|_v\}^{[K_v:\mathbb{Q}_v]} \prod_{\substack{v \nmid \infty \\ v(\mathfrak{b}) < 0}} \max\{1, |\beta|_v\}^{[K_v:\mathbb{Q}_v]} \\ &\geq \prod_{v|\infty} |\beta|_v^{[K_v:\mathbb{Q}_v]} \prod_{\substack{v \nmid \infty \\ v(\mathfrak{b}) < 0}} |\beta|_v^{[K_v:\mathbb{Q}_v]} = \prod_{\substack{v \nmid \infty \\ v(\mathfrak{b}) \geq 0}} |\beta|_v^{-[K_v:\mathbb{Q}_v]}, \end{aligned}$$

where the last equality follows from the product formula. Let  $e_{\mathfrak{p}}$  be such that  $\mathfrak{b} = \prod \mathfrak{p}^{e_{\mathfrak{p}}}$ . Since  $\beta \in \mathfrak{b}$ ,  $v(\beta) \geq e_{\mathfrak{p}_v}$ , so  $|\beta|_v^{-[K_v:\mathbb{Q}_v]} \geq N(\mathfrak{p}_v)^{e_{\mathfrak{p}_v}}$ .  $\square$

**Lemma 4.6.** *Let  $\mathfrak{a} \subset \mathcal{O}_K$  be an integral ideal, and let  $\rho_{\mathfrak{a}}: \mathbb{P}^n(\mathcal{O}_K) \rightarrow \mathbb{P}^n(\mathcal{O}_K/\mathfrak{a})$  denote the canonical projection. For each  $\beta = (\beta_0 : \beta_1 : \dots : \beta_n) \in \mathbb{P}^n(\mathcal{O}_K/\mathfrak{a})$ , there is at most one element  $\alpha = (\alpha_0 : \alpha_1 : \dots : \alpha_n) \in \rho_{\mathfrak{a}}^{-1}(\beta)$  with  $H_K(\alpha) < (2^{-[K:\mathbb{Q}]}N(\mathfrak{a}))^{1/2}$ .*

*Proof.* Let  $\alpha, \alpha' \in \mathbb{P}^n(\mathcal{O}_K)$  be such that  $H_K(\alpha), H_K(\alpha') < (2^{-[K:\mathbb{Q}]}N(\mathfrak{a}))^{1/2}$  and such that  $\rho_{\mathfrak{a}}(\alpha) = \rho_{\mathfrak{a}}(\alpha')$ . Since  $\alpha \in \mathbb{P}^n(\mathcal{O}_K)$ , there exists a coordinate  $i_0$  such that  $\alpha_{i_0} \notin \mathfrak{a}$ . It follows that  $\alpha'_{i_0} \notin \mathfrak{a}$  too.

Then for each  $i$  and each place  $v$ , an argument as in Proposition 4.3 shows that

$$\max \left\{ 1, \left| \frac{\alpha_i}{\alpha_{i_0}} - \frac{\alpha'_i}{\alpha'_{i_0}} \right|_v \right\} \leq 2 \max_{\ell} \left\{ \left| \frac{\alpha_{\ell}}{\alpha_{i_0}} \right|_v \right\} \cdot \max_{\ell} \left\{ \left| \frac{\alpha'_{\ell}}{\alpha'_{i_0}} \right|_v \right\}.$$

Taking the product over all  $v$  gives  $H_K \left( \frac{\alpha_i}{\alpha_{i_0}} - \frac{\alpha'_i}{\alpha'_{i_0}} \right) \leq 2^{[K:\mathbb{Q}]} H_K(\alpha) H_K(\alpha')$ . The latter is less than  $N(\mathfrak{a})$  by hypothesis, and  $\frac{\alpha_i}{\alpha_{i_0}} - \frac{\alpha'_i}{\alpha'_{i_0}}$  lies in the fractional ideal  $(\alpha_{i_0} \alpha'_{i_0})^{-1} \mathfrak{a}$ , so the preceding lemma implies that  $\frac{\alpha_i}{\alpha_{i_0}} = \frac{\alpha'_i}{\alpha'_{i_0}}$ . That is,  $\alpha = \alpha'$ .  $\square$

**Proposition 4.7.** *Let  $v_0, \dots, v_n$  be finite places of  $K$  such that*

- (1) *the reduction map  $\text{Aut}_{\phi}(K) \rightarrow \text{Aut}_{\phi}(\mathbb{F}_{v_i})$  is injective for all  $i$ , and*
- (2)  *$\prod_i N(v_i) \geq 2^{[K:\mathbb{Q}]} M^2$ , where  $M = 6^{[K:\mathbb{Q}]} L_2(f_T)^6$  is as in Corollary 4.4.*

*For any tuple  $(g_i) \in \prod_i \text{Aut}_{\phi}(\mathbb{F}_{v_i})$ , let  $g_K \in \text{Aut}(\mathbb{P}_K^1)$  be a simultaneous lift of each  $g_i$  of minimal height. If  $g_K \notin \text{Aut}_{\phi}(K)$ , then  $(g_i) \notin \text{im}(\text{Aut}_{\phi}(K) \rightarrow \prod_i \text{Aut}_{\phi}(\mathbb{F}_{v_i}))$*

*Proof.* Assume that  $(g_i) \in \text{im}(\text{Aut}_{\phi}(K) \rightarrow \prod_i \text{Aut}_{\phi}(\mathbb{F}_{v_i}))$  and let  $g' \in \text{Aut}_{\phi}(K)$  denote its pre-image. (The automorphism  $g'$  is unique by assumption (1).) By Corollary 4.4,  $H_K(g') \leq M \leq (2^{-[K:\mathbb{Q}]} \prod_i N(v_i))^{1/2}$ . By Lemma 4.6,  $g'$  must have minimal height among all lifts, so  $g' = g_K \in \text{Aut}_{\phi}(K)$ .  $\square$

There are a few technical details that we have left out in our description of Algorithm 4, mostly in the step where we decide whether to terminate and in the Chinese Remainder Theorem step. These details allow us to avoid extraneous computation. We give an example here and the curious reader can find the rest in the source code.

It is possible for the reduction of  $\text{Aut}_{\phi}(K)$  to be a proper subgroup of  $\text{Aut}_{\phi}(\mathbb{F}_v)$  for all places  $v$  of good reduction. Consider the rational map  $\phi = 2z^5$ . One can use the method of invariant sets to check that

$$\text{Aut}_{\phi}(\overline{\mathbb{Q}}) = \left\{ z, iz, -z, -iz, (\sqrt{2}z)^{-1}, i(\sqrt{2}z)^{-1}, -(\sqrt{2}z)^{-1}, -i(\sqrt{2}z)^{-1} \right\},$$

**Algorithm 4** — Computation of  $\text{Aut}_\phi(K)$  via the Chinese Remainder Theorem

---

Input: a number field  $K$  and a rational function  $\phi \in K(z)$  of degree  $d > 1$ 

Output: the set  $\text{Aut}_\phi(K)$ 

choose  $T$  as in Algorithm 2 and set  $M = 6^{[K:\mathbb{Q}]} L_2(f_T)^6$ 

create an empty list  $L$ , and set  $\mathfrak{a} = \langle 1 \rangle$ 

for  $v$  a prime of good reduction at  $v$  such that  $\text{Aut}_\phi(K) \rightarrow \text{Aut}_\phi(\mathbb{F}_v)$  is injective:

    compute  $\text{Aut}_\phi(\mathbb{F}_v)$  using Algorithm 3

    if  $\text{Aut}_\phi(\mathbb{F}_v) = \{z\}$ :

        return  $\{z\}$ 

else:

        append  $\text{Aut}_\phi(\mathbb{F}_v)$  to  $L$ , and set  $\mathfrak{a} = \mathfrak{a} \mathfrak{p}_v$ 

Set  $L' = CRT(L)$  and initialize an empty list  $\text{Auts}$ 

for  $s$  in  $L'$ :

    set  $s' \in \text{PGL}_2(\mathcal{O}_K)$  to be a lift of  $s$  of minimal height

    if  $H_K(s') \leq M$  and  $s' \circ \phi = \phi \circ s'$ :

        append  $s'$  to  $\text{Auts}$ 

if  $N(\mathfrak{a}) \geq 2^{[K:\mathbb{Q}]} M^2$  or if  $\#\text{Auts} = \#\text{Aut}_\phi(\mathbb{F}_v)$  for any  $v \mid \mathfrak{a}$ :

    return  $\text{Auts}$ 


---

which is a dihedral group of order 8. For all primes  $p > 2$ , at least one of  $-1, 2, -2$  is a square in  $\mathbb{F}_p$ . Therefore,  $\text{Aut}_\phi(\mathbb{F}_p)$  always contains  $\mathbb{Z}/2 \times \mathbb{Z}/2$  or  $\mathbb{Z}/4$  as a subgroup. As the algorithm is stated, we would compute a lift of every element in  $\prod_{p=5}^{19} \text{Aut}_\phi(\mathbb{F}_p)$ . However, by  $p = 7$  one can already recognize that  $\text{Aut}_\phi(\mathbb{Q}) \subseteq \mathbb{Z}/2$  since  $\text{Aut}_\phi(\mathbb{F}_5) = \mathbb{Z}/4$  and  $\text{Aut}_\phi(\mathbb{F}_7) = \mathbb{Z}/2 \times \mathbb{Z}/2$ . Our code checks for group-theoretic properties like this when deciding whether to terminate.

It is important to build in as many early termination conditions as possible, since typically the elements of  $\text{Aut}_\phi(K)$  have significantly smaller height than the theoretical bound. This is of course true when  $\text{Aut}_\phi(K)$  is trivial, but it remains true even in the non-trivial case. For example, consider the functions in the last 3 lines of Table 1. The height bound for  $\phi = 345025251z^6$  is over 50 digits, and the height bounds for the other two are over 100 digits. In contrast, the heights of the automorphisms are (from last to first) 2601, 101 and 11.

## 5. EXAMPLES

In this section, we compute some examples to give an idea of the running time. It is hard to produce “random” examples that have non-trivial automorphism group. Therefore, we present some hand-selected examples with non-trivial automorphism group which demonstrate the correctness of the algorithm (see Table 1). Then we present median running times for randomly generated rational maps of varying degrees and varying heights (see Table 2). All of the randomly generated functions had trivial automorphism group.

Our computations indicate that the fixed-point method is faster for rational functions of small degree, but that the CRT method is a better choice once the degree is larger than 15. In our implementation, the main bottleneck in the fixed point algorithm is in computing  $Z_{1,2}$  and  $Z_{2,2}$ ; this requires computing the quadratic factors of a degree  $d^2 + 1$  polynomial. It is possible that the fixed-point method

$\phi$	CPU time		$\text{Aut}_\phi(\mathbb{Q})$
	CRT	FP	
$\frac{z^2-2z-2}{-2z^2-2z+1}$	0.338825	0.058	$z^{\pm 1}, \left(\frac{-z}{z+1}\right)^{\pm 1}, (-z-1)^{\pm 1}$
$\frac{z^2-4z-3}{-3z^2-2z+2}$	0.101023	0.020238	$z, \frac{-z-1}{z}, \frac{-1}{z+1}$
$\frac{z^5-5z^4+10z^2-5z}{-5z^4+10z^3-5z+1}$	2.445185	0.205686	$z, \frac{z}{z-1}, -z+1, \frac{1}{z}, \frac{2z-1}{z-2}, \frac{-z+2}{z+1},$ $\frac{z-2}{2z-1}, \frac{z+1}{2z-1}, \frac{-1}{z-1}, \frac{z-1}{z}, \frac{-z-1}{z-2}, \frac{2z-1}{z+1}$
$\frac{z^5-20z^4+30z^3+10z^2-20z+3}{-3z^5-5z^4+40z^3-30z^2-5z+4}$	0.583004	0.035206	$z, \frac{z-2}{2z-1}, \frac{-1}{z-1}, \frac{z-1}{z}, \frac{-z-1}{z-2}, \frac{2z-1}{z+1}$
$\frac{3z^2-1}{z^3-3z}$	0.227719	0.042237	$\pm z, \pm \frac{1}{z}, \pm \left(\frac{-z+1}{z+1}\right), \pm \left(\frac{z+1}{z-1}\right)$
$\frac{z^3-21z^2-3z+7}{-7z^3-3z^2+21z+1}$	0.648	0.024699	$z, \frac{-1}{z}, \frac{z-1}{z+1}, \frac{-z-1}{z-1}$
$\frac{z^{11}+66z^6-11z}{-11z^{10}-66z^5+1}$	0.676026	0.069261	$z, -1/z$
$32z^5$	0.681829	0.035364	$\pm z$
$\phi = (z^{-18})^f, f = \frac{-10z-2}{z-7}$	1.663506	2.962213	$z, \frac{-3z+5}{11z+3}$
$\phi = (z^{19})^f, f = \frac{-10z-2}{z-7}$	43.554845	4.678652	$z, \frac{-17z-7}{-5z+17}, \frac{-3z+5}{11z+3}, \frac{-13z-53}{101z+13}$
$345025251z^6$	337.721855	0.073642	$z, 1/(2601z)$

TABLE 1. Running times for `automorphism_group_QQ` on rational functions with non-trivial automorphism group.

can be made feasible for larger degrees by implementing a faster method for finding quadratic factors of large degree polynomials.

These examples were computed on a Macbook Air (Apple, Inc.) running Mac OS X 10.7.2 with a 2.13 GHz Intel Core 2 Duo processor and 2GB of RAM. They were run with Sage 4.7.2 which was released on October 29, 2011. All running times are listed in seconds.

## 6. CONJUGATE RATIONAL FUNCTIONS

Let  $F$  be a number field or finite field, and let  $\phi, \psi : \mathbb{P}_F^1 \rightarrow \mathbb{P}_F^1$  be a pair of endomorphisms of the same degree  $d$ . We return now to the question presented in the introduction:

Does there exist a change of coordinate  $f \in \text{PGL}_2(F)$  such that  $\psi = f \circ \phi \circ f^{-1}$ ; i.e., are  $\phi$  and  $\psi$  conjugate over  $F$ ?

This question can be dealt with both theoretically and computationally in a manner similar to that of automorphism groups. We briefly sketch the theoretical side; the proofs are straightforward modifications of arguments presented earlier.

**Definition.** Fix a nonnegative integer  $d$ , and let  $\phi, \psi : \mathbb{P}_R^1 \rightarrow \mathbb{P}_R^1$  be two endomorphisms of degree  $d$ . The **conjugation scheme** of the pair  $(\phi, \psi)$  is the  $R$ -scheme  $\text{Conj}_{\phi, \psi}$  represented by the functor  $\underline{\text{Conj}}_{\phi, \psi} : R\text{-Alg} \rightarrow \mathbf{Grp}$  defined by

$$\underline{\text{Conj}}_{\phi, \psi}(S) = \{f \in \text{Aut}(\mathbb{P}_S^1) : f \circ \phi \circ f^{-1} = \psi\}.$$

	d	Height Bound					
		50	10 <sup>2</sup>	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>5</sup>	10 <sup>6</sup>
Fixed Point	3	0.0124450	0.0133855	0.0133215	0.0132855	0.0127770	0.0129115
	6	0.0254290	0.0263755	0.0270010	0.0270970	0.0294735	0.0307725
	9	0.0773140	0.0808070	0.0807205	0.0908770	0.0938780	0.0961555
	12	0.282548	0.2629635	0.2917585	0.2940025	0.3132295	0.3472265
	15	0.980427	1.0104325	1.0165010	1.0359760	1.1184880	1.1377990
CRT	10	0.1932860	0.1968665	0.2083450	0.2070960	0.2180315	0.2347400
	15	0.5662205	0.5173635	0.5148960	0.5360245	0.4533855	0.5041420
	20	1.8513510	1.9718745	1.9562015	1.7734270	1.9558800	1.9808705
	30	17.702872	18.402277	17.750321	20.359524	18.483440	18.752402
	40	106.19608	102.52844	106.19090	113.88063	113.06002	122.07266

TABLE 2. Median running times for the fixed point and CRT algorithms on 100 random rational functions with given degree and height bound.

**Theorem 6.1.** *Let  $R$  be a commutative ring, let  $d \geq 0$  be an integer, and let  $\phi, \psi : \mathbb{P}_R^1 \rightarrow \mathbb{P}_R^1$  be endomorphisms of degree  $d$ . Then the functor  $\text{Conj}_{\phi, \psi}$  is represented by a closed  $R$ -subscheme  $\text{Conj}_{\phi, \psi} \subset \text{PGL}_2$ . If moreover  $d \geq 2$ , then  $\text{Conj}_{\phi, \psi}$  is finite over  $\text{Spec } R$ .*

The theorem does not preclude the possibility that  $\text{Conj}_{\phi, \psi}$  is the empty scheme; in fact, it is typically empty when  $d \geq 2$ . The group scheme  $\text{PGL}_2$  has relative dimension 3 over  $R$ , and the space  $\text{Rat}_d$  of endomorphisms of  $\mathbb{P}^1$  of degree  $d$  has relative dimension  $2d + 1 > 3$  over  $R$ . So for a fixed  $\phi \in \text{Rat}_d(R)$ , a general choice of  $\psi$  will yield  $\text{Conj}_{\phi, \psi} = \emptyset$ .

*Remark 6.2.* When  $\text{Conj}_{\phi, \psi}$  is not the empty scheme, it is a principal homogeneous space for  $\text{Aut}_{\phi}$  (or  $\text{Aut}_{\psi}$ ).

In the case  $d \geq 2$  of the theorem, in order to establish that  $\text{Conj}_{\phi, \psi}$  is finite over  $\text{Spec } R$ , one must argue that it is proper and quasi-finite. Properness follows from a direct generalization of the Reduction Lemma. Quasi-finiteness may be proved by taking  $R = F$  to be an algebraically closed field and using a variation of our method of invariant sets in §4.1. The basic idea is to replace the invariant set  $T$  with two sets  $T_{\phi}, T_{\psi} \subset \mathbb{P}^1(F)$  such that

- $\#T_{\phi} \geq 3$ , and
- $s(T_{\phi}) \subset T_{\psi}$  for every  $s \in \text{Conj}_{\phi, \psi}(F)$ .

The sets  $T_{\phi}, T_{\psi}$  may be taken as the fixed points of  $\phi$  and  $\psi$ , respectively; if there are not enough fixed points, then one may use pre-images exactly as in Algorithm 1. We leave the details to the reader.

Finally, we note that the algorithms in §4.1 and §4.3 may be adapted (as in the previous paragraph) to give algorithms for computing  $\text{Conj}_{\phi, \psi}(F)$  and  $\text{Conj}_{\phi, \psi}(\bar{F})$  when  $F$  is a finite field or number field. Again, we leave the details to the interested reader; note that the main technical tool — Proposition 4.3 — applies in this more general situation. We close with the remark that, in particular, this strategy gives an algorithmic procedure for determining if  $\text{Conj}_{\phi, \psi}$  is the empty scheme or not. More concretely, this means that one can determine effectively if two rational functions  $\phi$  and  $\psi$  are conjugate.



## REFERENCES

- [1] Daniel S. Alexander. *A history of complex dynamics*. Aspects of Mathematics, E24. Friedr. Vieweg & Sohn, Braunschweig, 1994. From Schröder to Fatou and Julia.
- [2] Eric Bach. Toward a theory of Pollard's rho method. *Inform. and Comput.*, 90(2):139–155, 1991.
- [3] Matthew Baker and Robert Rumely. *Potential theory and dynamics on the Berkovich projective line*, volume 159 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2010.
- [4] Arnaud Beauville. Finite subgroups of  $\mathrm{PGL}_2(K)$ . In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.
- [5] Xander Faber. Finite  $p$ -irregular subgroups of  $\mathrm{PGL}_2(k)$ . Preprint, arXiv:1112.1999v1 [math.NT], 2011.
- [6] Xander Faber. Topology and geometry of the Berkovich ramification locus for rational functions. Preprint, arXiv:1102.1432v3 [math.NT], 2011.
- [7] Xander Faber and Andrew Granville. Prime factors of dynamical sequences. To appear in *J. Reine Angew. Math.*
- [8] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
- [9] Marc Hindry and Joseph H. Silverman. *Diophantine geometry. An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [10] Mattias Jonsson. Dynamics on Berkovich spaces in low dimensions. Preprint, arXiv:1201.1944v1 [math.DS], 2012.
- [11] John Milnor. *Dynamics in one complex variable*. Friedr. Vieweg & Sohn, Braunschweig, second edition, 2000. Introductory lectures.
- [12] Clayton Petsche, Lucien Szpiro, and Michael Tepper. Isotriviality is equivalent to potential good reduction for endomorphisms of  $\mathbb{P}^N$  over function fields. *J. Algebra*, 322(9):3345–3365, 2009.
- [13] J. M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)*, 15(3):331–334, 1975.
- [14] Juan Rivera-Letelier. Points périodiques des fonctions rationnelles dans l'espace hyperbolique  $p$ -adique. *Comment. Math. Helv.*, 80(3):593–629, 2005.
- [15] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [16] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [17] W. A. Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2009. <http://www.sagemath.org>.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII AT MĀNOA, HONOLULU, HI  
*E-mail address*: xander@math.hawaii.edu, mmanes@math.hawaii.edu

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RI  
*E-mail address*: bviray@math.brown.edu